Preventing the Compromise of Classified Data on DON IT Systems and Networks

By Jennifer Korenblatt

Introduction

This article discusses the responsibilities of Department of the Navy (DON) information technology (IT) users for protecting classified information on DON IT systems and networks. Classified data exist in both a physical and electronic state. While physical protection of classified information is critical regardless of media, this article primarily focuses on protecting classified data residing on IT systems.

Classified information is so designated by the U.S. government based on the amount of harm to national security that would occur if unauthorized individuals obtain it. There are three levels of classified information:

CONFIDENTIAL – *some damage to national security would occur*
SECRET – *serious damage to national security would occur*
TOP SECRET – *exceptionally grave damage to national security would occur as defined by the Department of Defense (DoD) 5220.22-M, National Industrial Security Program Operating Manual.*

To understand the importance of information security, it is important to understand several key security definitions. Information security refers to the protection of information and information systems from "unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide" integrity, confidentiality and availability of the information as defined by the Federal Information Security Management Act (FISMA) of 2002.

A security compromise refers to the unauthorized disclosure of classified information to a person(s) who does not have a valid clearance, authorized access or a need-to-know. A compromise can occur when classified information is not properly controlled as defined in FISMA. Other terms often used for compromise are: classified information spillage, unauthorized disclosure and system contamination. A compromise can also occur if data of a higher classification is disclosed to a system or network only approved to process information at a lower classification level (i.e., top secret information disclosed onto a secret system, secret information disclosed onto a confidential system, etc.).

Information technology includes, but is not limited to, telephones (including cell phones), computers and workstations, information and communication systems, software, networks, pagers, fax machines, personal digital assistants (PDAs), Internet access and e-mail.

The Problem

The DON increasingly depends on IT to conduct mission functions. This dependence increases the DON's vulnerability to the mishandling of classified information on its systems and networks. The compromise of classified secret information onto unclassified systems and networks is a growing problem in the DON. A new Navy Marine Corps Intranet (NMCI) Contract Line Item Number (CLIN), NMCI CLIN 0046, "File Removal Service," issued Jan. 19, 2005, allows the NMCI vendor to charge commands for file removal service of each compromise of classified information on the NMCI.

Costs can be as high as $11,800 for just one compromise incident. The DON must prevent compromises to avoid significant costs and lost productivity. It can take up to three weeks to resolve a compromise incident, so each compromise affects the security of DoD and DON mission functions. DON users are the first line of defense for protecting information on DON networks and systems. However, one of the greatest threats to the information security posture of any system is the insider threat. So it is imperative for all DON IT system users to increase awareness of individual responsibility to safeguard classified information.

Compromise Incident Examples

How does a compromise of classified information occur? Consider the following scenarios.

Scenario: It is 1600 on Friday afternoon; your boss sends you a classified secret document via SIPRNET asking you to review it as soon as possible. With your mind on your dinner reservation you decide to save the document to a disc so you can work at home. You save the secret document on a disc in a classified secret computer, insert the disc into an unclassified computer, upload the document to your unclassified system and e-mail the document to your personal e-mail account.

Result: You have just compromised classified information, and the consequences will ruin more than your dinner plans. What happened? You processed secret information on an unclassified system and did not apply proper security controls to classified data. You e-mailed secret information over the NIPRNET, which is not an authorized network to process secret information. Sending secret information to an unclassified, personal e-mail account is the unauthorized dissemination of classified information via an unclassified e-mail (either within the body of the e-mail or as an attachment).

Clear text sent over the Internet is available for anyone to read. Sending DoD classified information over the Internet exposes the information to unofficial release to the public. A public media compromise is the unofficial release of DoD classified information to the public resulting in its unauthorized disclosure.

Prevent compromise by: (1) Marking and protecting media according to the security classification level of the data residing on the media per Secretary of the Navy Instruction (SECNAVINST)

5510.36, DON Information Security Program (ISP) Regulation and the Defense Information Systems Agency (DISA) Information Assurance Security Awareness Briefing; (2) Remembering that classified information should be afforded a level of control commensurate with its assigned security classification level; and (3) Never sending DoD classified information over the NIPRNET or Internet.

Scenario: You pick up a disc with messages from the data center. You are sure the disc contains only unclassified messages despite its being labeled as secret. You place the disc with a secret label into the disc drive of an unclassified system. Lo and behold, the disc contains a secret classified message, and you just uploaded it to an unclassified system.

Result: Uploading classified secret information onto an unclassified system causes a compromise of classified data. This incident occurred through improper handling of marked classified material. Prevent this compromise by observing security classification markings on media and protecting media accordingly.

Everyone's Responsibility

Every DON military, civilian and contractor employee has a responsibility to protect the availability, integrity and confidentiality of DON IT assets. While most security breaches are not deliberate, intentional misuse of classified information is a crime. The Computer Fraud and Abuse Act (CFAA) lists the crimes associated with actions such as gathering, transmitting or losing defense information and disclosure of classified information.

Computer crimes are serious, and the punishment for offenses ranges from fines to imprisonment for up to 20 years. While the majority of compromises of classified information are unintentional, the consequences remain serious. Authorized users can do the most damage to a system or network through mistakes and mishandling information. We must remain vigilant and use sound information assurance (IA) practices when using DON systems, and pay special attention to actions that involve use of the Internet and moving data between different security classification levels.

Training

In addition to federal law, DoD and DON policies require users of DoD information systems to receive IA training commensurate with their duties as a condition of system access. DON annual IA training is not only mandatory, but it is an opportunity to reinforce knowledge of sound security practices for safeguarding all classifications of information. The goal of the training is to make sure all DON personnel who use DON information systems know the risks associated with their day-to-day activities, their individual responsibilities to meet the requirements of laws, policies and procedures, and the best security practices to use to reduce risks.

Each command is responsible for providing IA awareness training and ensuring all personnel understand their responsibilities for safeguarding classified information. If you have not received this training, speak to your security manager immediately. Standardized IA awareness training is available to Navy users through Navy Knowledge Online at http://www.nko.navy.mil and Marine users through MarineNet at http://www.marinenet.usmc.mil. Training must be completed by Sept. 1, 2005, for all authorized DoD users.

Resources

• Free information assurance training products are available upon request from the DoD IA Portal at http://iase.disa.mil/. The DoD IA Portal also has a link to the DISA Information Awareness Security Briefing.

• Computer Fraud and Abuse Act (CFAA) Title 18 PT1, Chap. 47 § 1030 (a)

• Defense Security Service (DSS), http://www.dss.mil

• Federal Information Security Management Act of 2002, available at http://www.csrc.nist.gov/policies/FISMA-final.pdf

The following can be accessed from the Policy and Guidance tab of the DON CIO Web site at http://www.doncio.navy.mil

• DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), January 1995

• DoDD 8500.1, Information Assurance (IA), Oct. 24,2002

• DoD Instruction (DoDI) 8500.2, Information Assurance (IA) Implementation, Feb. 6, 2003

• DoDD 8570.1, Information Assurance Training, Certification and Workforce Management, Aug. 15, 2004

• SECNAVINST 5510.36, Department of the Navy (DON) Information Security Program Regulation, March 17, 1999

• SECNAVINST 5239.3A, DON IA Policy, December 2004

What To Do If Classified Data Is Compromised

Individuals who become aware of the loss or compromise of classified information must immediately notify their commanding officer or security manager of the incident. DON users who discover a compromise on an NMCI system or network shall immediately cease operation on the affected system and contact the NMCI Help Desk (Toll Free: 1-866-843-6624) and their command information assurance manager or designated personnel. SECNAVINST 5510.36, Chapter 12, details reporting responsibilities for both individuals and commanding officers upon loss or compromise of classified information.

DoD and DON information technology users are responsible for protecting classified information and knowing which security controls are required to protect classified data. By applying controls continuously and complying with applicable regulations, we can protect classified data and help ensure the integrity, protection and security of DON IT systems and equipment.

Jennifer Korenblatt is a member of the Department of the Navy Chief Information Officer (DON CIO) Information Assurance Team. CHIPS